National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

NSF 17-019

Dear Colleague Letter (DCL): Enabling New Collaborations Between Computer and Information Science & Engineering (CISE) and Social, Behavioral and Economic Sciences (SBE) Research Communities

With this DCL, the National Science Foundation (NSF) is announcing its intention to build upon the success of previous EArly-Concept Grants for Exploratory Research (EAGERs) in the areas supported by the Secure and Trustworthy Cyberspace (SaTC) program (see NSF 16-580, https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf16580&org=NSF) and to encourage the submission of additional EAGER proposals that foster novel interdisciplinary research carried out in new collaborations between one or more Computer and Information Science and Engineering (CISE) researchers *and* one or more Social, Behavioral and Economic Sciences (SBE) researchers. Note that this DCL is focused on *new* collaborations; research teams with a history of collaborating together should instead submit directly to the SaTC solicitation, pursuant to the proposal preparation guidelines specified therein.

Many scientific and practical challenges of security, privacy, and trust have sociotechnical dimensions, and thus it is important to encourage interdisciplinary collaborations among researchers from the disciplines represented in NSF's CISE and SBE directorates, and on topics that draw on the strengths of each researcher.

Below are some examples of the types of topics that might benefit from collaborations between CISE and SBE researchers under such an EAGER project. This list is by no means intended to be directive or complete. Many important problems demand strong research reflecting integrative perspectives.

- Ethical, political, legal, cultural, or societal dimensions of security and privacy technologies and their impacts.
- Security/privacy in the context of social media, including topics such as data aggregation and algorithmic filtering.
- Addressing online behavioral risks to security, safety, and/or privacy, including trolling, spamming and cyberbullying.
- Interaction design research on how to accommodate individual and/or collective privacy values and concerns.
- Inclusive security or privacy mechanisms that adapt to the needs and abilities of underrepresented or disabled individuals or groups.
- Research on education, training, and awareness around security and privacy for both users and developers of secure and trustworthy systems.
- Understanding and supporting responses to cyberattacks, ranging from the individual to national scales.
- Security/privacy at the level of families, groups, communities, and other understudied levels/units of analysis.
- Organizational strategies, investments, or governance effects on security/privacy, and approaches for improvement.
- Studies of economic dimensions of security or privacy decision-making, including cost-benefit

analyses, incentive structures, and/or mechanism design.
- Methods for modeling intentions and/or behaviors relevant to cybersecurity. For example, methods could include social network analysis, crowdsourcing, and inter-organizational policy analysis, and combinations thereof.

Proposals submitted pursuant to this DCL must include one or more PIs from the fields supported by the Computer and Information Science and Engineering (CISE) directorate, and one or more PIs from those areas supported by the Social, Behavioral, and Economic sciences (SBE) directorate. Proposals should describe how intellectual merit and broader impacts will benefit from the contribution from each discipline. Proposals where one side is mainly in service of the other are not appropriate. Ideally, the research will be interdependent and integrated-sharing visions, models, methods, or discoveries. Such integration may require extra effort in leadership, regular communication, and cross-training. Proposals must also describe how the collaboration will work in the planning, research, and dissemination stages.

Two rounds of submissions are anticipated, with approximately five EAGERs awarded during each round, subject to the availability of funds. The anticipated deadlines for submission of EAGER proposals are December 1, 2016, and April 1, 2017, for the first and second rounds, respectively.

Submission of EAGER proposals will be via Fastlane or Grants.gov. EAGER submissions should follow the NSF's Proposal and Award Policies and Procedures Guide (PAPPG; https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf16001). As noted in the PAPPG, EAGER is a funding mechanism for supporting exploratory work in its early stages on untested, but potentially transformative, research ideas or approaches. Thus, proposals must talk about why they are appropriate for an EAGER (for instance, proposals that respond to this solicitation may be “high-risk, high-reward” through involving radically different approaches, applying new expertise, or engaging novel disciplinary or interdisciplinary perspectives).

An investigator may be included in only one submission (across both rounds) pursuant to this DCL; if more than one is submitted, only the first one submitted will be considered. Submission pursuant to the previous CISE/SBE SaTC EAGER DCLs does not preclude submission in response to this DCL.

For further information, please contact the following SaTC program directors: Drs. Sara Kiesler (skiesler@nsf.gov), Nan Zhang (nanzhang@nsf.gov), and Dan Cosley (dcosley@nsf.gov).

Sincerely,

Jim Kurose
Assistant Director, CISE

Fay Lomax Cook
Assistant Director, SBE